ICIT 2023

The 24th IEEE International Conference on Industrial Technology

Orlando FL, USA | 4 - 6 April, 2023

IEEE


# ICIT 2023 Special Session Proposal

**Title of the Proposal:** Cybersecurity of Industry Applications powered by 5G's capability of massive machine type communications (mMTC)

**Technical Outline of the Session and Topics:**

Outline of the Session:

Industry 4.0 transformation includes massive machine type communications (mMTC) for IoT services made possible by 5G. It includes integration of different platforms such as cloud and fog/edge computing platforms in handling the heterogeneous and numerous IoT traffic generated in the network of 5G and 6G/Future G. This session will bring together researchers working not only on improving the network infrastructure to accommodate IoT and/or mMTC services but also on realizing secure real-time IoT services in various domains such as factories, warehouses, smart cities, smart grid, vehicular networks, underwater networks, and so on. Sharing of new ideas, work in progress, latest findings, and results are invited on the following mMTC & IoT and other related topics.

Topics of the Session:

- Securing mMTC services in 5G and 6G/Future G for Industrial applications
- Softwarization of next generation mMTC networks
- Slicing to support heterogeneous mMTC services
- Network function virtualization (NFV) in the context of industrial services
- ML and AI for enabling real-time IoT/mMTC services
- Integration of cloud-edge infrastructure with 5G/6G/Future G
- Enabling heterogeneous and sporadic mMTC services using vehicular networks
- Smart grid communication for heterogeneous and sporadic mMTC services
- Network resource allocation and management in Industrial mMTC networks
- Network strict-QoS for Industrial applications

**IEEE IES Technical Committee Sponsoring the Special Session (if any): TBD**

**Short bio and contact details of the Session Organizers**

Arupjyoti (Arup) Bhuyan is the Director of the Wireless Security Institute in the Idaho National Laboratory. The focus of his research is on secure implementation of future generations of wireless communications with scientific exploration and engineering innovations across the fields of wireless technology, cybersecurity, and computational science. Specific goals are to lead and focus wireless security research efforts for 5G and NextG/6G with national impact, to secure 5G spectrum sharing with distributed scheduling, and communication for a nationwide unmanned aerial system. Arup has extensive industry experience in wireless communications from his work before he joined INL in October 2015. He received his Ph.D. in Engineering and Applied Sciences from Yale University. He is a senior member of IEEE.

Amitabh Mishra is a Senior Wireless Security Researcher with INL Wireless Security Institute pursuing security of 5G cellular network infrastructure and applications. Before joining INL he was he was associated with the Office of Undersecretary of Defense for Research and Engineering – 5G-Next G initiative as a Senior Technical Lead for Beyond 5G and Operate Through Programs, and a Principal Engineer, Space and Terrestrial Communication Directorate, US Army CERDEC, Aberdeen Proving Ground, MD where he was leading teams in Machine Learning/ Artificial Intelligence, Data Science, and 5G communications to modernize the Army Tactical Wireless Networks. In the past he has been an Affiliated Professor in the Electrical and Computer Engineering Department at the University of Delaware, Research Assistant Professor in the Department of Computer Science at Johns Hopkins University, and Associate Professor in the Electrical and Computer Engineering Department, Virginia Tech researching wireless sensor and dynamic spectrum access networks and network security. Prior to coming to academia, he was a member of technical staff with AT&T and Lucent Bell Laboratories where he worked on architecture and performance of distributed memory multi-processor architectures, and 5ESS switch supporting cellular wireless communication networks. Amitabh obtained Ph. D. in Electrical & Computer Engineering from McGill University, and MS in Computer Science from the University of Illinois. He is a senior member of IEEE and a member of ACM.

Milos Manic is a professor with the Computer Science Department at Virginia Commonwealth University and is the director of the VCU Cybersecurity Center. He is also a Commonwealth Cyber Initiative Fellow, inaugural class 2020-2022. As a principal investigator or university partner, he has completed more than 40 research grants with the departments of Energy, Homeland Security, Air Force, Battelle Energy Alliance/Idaho National Laboratory, National Science Foundation, and industry entities, in the area of data mining and machine learning applied to cybersecurity, critical infrastructure protection, energy security, and resilient intelligent control. Manic has given over 40 invited talks around the world, authored more than 200 refereed articles in international journals, books, and conferences, holds several U.S. patents and won

the 2018 R&D 100 Award for Autonomic Intelligent Cyber Sensor (AICS), one of top 100 science and technology worldwide innovations in 2018. He is also an inductee of U.S. National Academy of Inventors (class of 2019). He is an IEEE Fellow, recipient of IEEE IES 2019 Anthony J. Hornfeck Service Award. He also received the 2012 J. David Irwin Early Career Award and 2017 IEM Best Paper Award. He serves as an associate editor of Transactions on Industrial Informatics, Open Journal of Industrial Electronics Society, and is IES Officer and Senior AdCom member. He served as associate editor of Trans. on Industrial Electronics, was a founding chair of IEEE IES Technical Committee on Resilience and Security in Industry, and a general chair of IEEE IECON 2018, IEEE HSI 2019.